3. *Зулькарнеев И. Р.*, *Тякунов М. С.*, *Кибардина Ю. А.* Объединение методик создания модели нарушителя по требованиям ФСТЭК и ФСБ // Безопасность информационного пространства. Курган : РИЦ Курган. гос. ун-та, 2016. С. 22–25.

4. *Бурькова Е. В.* Задача оценки защищенности информационных систем персональных данных // Вестн. Чуваш. ун-та. 2016. № 1. С. 112–118.

УДК 004.056

Ю. А. Кибардина
Научный руководитель: ст. преп. И. И. Пряхин
Тюменский государственный университет, Тюмень

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ, НЕ ЯВЛЯЮЩЕЙСЯ ИСПДн

Аннотация. В данной работе поднимается вопрос определения уровня защищенности информационной системы, не относящейся к информационной системе персональных данных или государственной информационной системе. Рассматривается возможность применения российского и зарубежных стандартов для оценки уровня защищенности такой информационной системы.

Ключевые слова: информационная безопасность; уровень защищенности; класс защищенности; информационная система; стандарт.

При работе на предприятии или в какой-либо организации руководство может поставить перед специалистом в области информационной безопасности вопрос, насколько защищенной является наша структура. По сути, в данном случае необходимо с помощью ряда показателей оценить общий уровень защищенности информационной системы (ИС). Российские регуляторы дают четкое разграничение для оценки уровня защищенности информационной системы персональных данных (ИСПДн), а также для государственных информационных систем (ГИС), для которых предусмотрены уровни и классы защищенности соответственно. Однако бывают случаи, когда ИС не относятся ни к ИСПДн, ни к ГИС. В таком случае законодательство Российской Федерации не предлагает четкой классификации для определения защищенности ИС. Поскольку оценка уровня защищенности «произвольной ИС» (далее будем называть произвольной такую ИС, которая не относится ни к ИСПДн, ни к ГИС) производится внутренними службами, исходя из внутренних требований к информационной безопасности, выработка единой методики несколько затрудняется.

Национальный стандарт РФ ИСО/МЭК 27001–2006 посвящен описанию модели процесса обеспечения информационной безопасности. Суть стандарта заключается в подходе к процессу обеспечения информационной безопасности организации как к непрерывному действию на протяжении всего времени существования ИС. Также данный стандарт предлагает описание этого процесса в виде модели PDCA, суть которой заключается в проведении периодической оценки рисков и их обработки. Одной из основных идей ИСО/МЭК 27001–2006 является необходимость определения специалистом службы информационной безопасности показателей рисков, при которых они могут быть приняты, при этом величину этого показателя выбирает служба безопасности организации и согласовывает со своим начальством самостоятельно, исходя из внутренних требований и ресурсов организации. Иными словами точного показателя для оценки не предлагает.

Далее был рассмотрен зарубежный стандарт NIST Special Publication 800-30. Данный стандарт полностью посвящен проблеме оценки рисков и разработки мероприятий по реагированию на них. Он предлагает совершенно иную модель обеспечения безопасности в организации. Она представляет собой также непрерывный процесс, содержащий в себе следующие элементы: определение «среды риска»; оценка риска; обработка риска; и мониторинг риска, при этом «среда риска» оказывает влияние на все остальные элементы процесса обеспечения безопасности. Основным отличием данного стандарта является построение сценариев риска, а также представление риска как совокупность угрозы и нескольких уязвимостей, а не как пару угроза-уязвимость, как предложено в ИСО/МЭК 27001–2006.

Следующим был рассмотрен стандарт ISF 2011 для информационной безопасности. Стандарт предлагает модель безопасности, состоящую из руководства, рисков, обязательств, людей, процессов и технологий, при этом каждый элемент представляет собой «треугольник», сторонами которого являются обмен знаниями, исследования и отчетность и средства и методы, обеспечивающие функционирование этих элементов. Сам стандарт предлагает ряд требований для тех или иных составляющих данной модели, т. е. предлагает перечень требований, которым организация и ИС должны соответствовать для обеспечения информационной безопасности предприятия.

Стандарт PCI о требованиях к безопасности данных также относится к информационной безопасности, как и стандарт ISF 2011, представляет собой набор требований, однако эти требования относятся именно к сохранности данных при их хранении, модификации, передаче и пр. Сам стандарт представляет собой таблицу с общими требованиями к технической составляющей процесса обработки данных. Оформлен в виде таблицы с формулировкой требования, процедурами тестирования и столбцом, называемым в английском варианте

как «руководство», но наиболее точным его смысловым переводом стал бы «комментарий». Несмотря на то, что стандарт предназначается для использования в платежных системах, для оценки уровня защищенности «произвольной ИС» он также может быть полезен.

И так, после рассмотрения всех вышеуказанных стандартов в области информационной безопасности, а также проведения их анализа, были сформированы рекомендации по использованию этих стандартов для определения уровня защищенности «произвольной ИС». Решено взять за основу стандарт ISF, так как он наиболее приближен к заданной цели. Используя предложенную данным стандартом модель безопасности, можно рассматривать по пунктам на соответствие каждому из требований для каждого составляющего этой модели для получения полной картины защищенности ИС к каждой из областей и в дальнейшем уже вести работы по устранению несоответствий именно в тех местах, где наиболее низок уровень защищенности. Для оценки суммарного уровня защищенности ИС можно использовать обобщенный показатель, вычисляемый исходя из уровней защищенности компонентов модели.

Стандарт PCI можно использовать в дополнение к элементу «Технологии» модели безопасности ISF для более точной оценки защищенности данного компонента. А стандарты ИСО/МЭК 27001–2006 и NIST 800-30 можно использовать для проверки элемента модели безопасности «Руководство».

Также ИСО и NIST подходят для проведения оценки рисков и работ по их обработке и нивелированию после проведения анализа уровня защищенности ИС, так как при низкий уровень защищенности, скорее всего, повлечет за собой работы по увеличению вычисленного показателя, что удобнее всего реализовать через прохождение процедуры оценки рисков. При этом одним из наиболее удобных вариантов комбинации данных стандартов может служить следующая вариация: использование стандарта ИСО/МЭК 27001–2006 как основного, а для рисков, считающихся приемлемыми, можно провести дополнительный анализ с использованием построения сценариев угроз и агрегации рисков, так как риск может оказаться приемлемым за счет низкой вероятности его возникновения или маленькой величины ущерба, однако низкая вероятность может быть обусловлена тем, что уязвимость реализуется только после реализации какой-либо другой уязвимости или ряда уязвимостей, а реализация самого риска может принести сама по себе небольшой ущерб, но повлечь за собой более легкую процедуру эксплуатации другого риска и/или не связанной с данным риском уязвимости.

Рассмотренные в данной статье стандарты являются стандартами, находящимися в общем доступе, свободно распространяемые в информационно-телекоммуникационной сети Интернет, что делает их доступными для рассмотрения и использования при построении и анализе защищенных ИС. Данная

статья предлагает один из множества способов их комбинации для обеспечения информационной безопасности, а в частности, определения уровня защищенности «произвольной ИС» и проведения работ по увеличению показателя защищенности этой ИС.

УДК 342.922/951

П. А. Криворотова
Научный руководитель: ст. преп. В. М. Жернова
Южно-Уральский государственный университет, Челябинск

ОБЗОР НОРМАТИВНО-ПРАВОВОЙ БАЗЫ В СФЕРЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье проводится обзор и анализ нормативных правовых документов, которые регламентируют деятельность по обеспечению безопасности критической информационной инфраструктуры Российской Федерации. Применение исторического метода в исследовании позволило провести анализ развития и создания системы ГосСОПКА.

Ключевые слова: критическая информационная инфраструктура; безопасность объектов.

Каждый год средства массовой информации публикуют все больше сообщений о кибератаках на объекты критической информационной структуры коммерческих компаний и государственных организаций. В ответ на угрозы было решено спроектировать и ввести в эксплуатацию государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

В 2013 г. Указом президента РФ от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [1] было постановлено возложить на Федеральную службу безопасности полномочия органа исполнительной власти по созданию системы ГосСОПКА.

Следующим шагом было утверждение Концепции № К 1274 12 декабря 2014 г. [2], в которой более конкретно определяются виды обеспечения, необходимые для ее создания и функционирования. В концепции был увеличен перечень осуществляемых системой функций, а также ее территориальная и отра-